CBC | IntoSAINT

Organizational Integrity Self-Assessment

IntoSAINT HANDBOOK

2026

TABLE OF CONTENTS

FOREWORD

Organizational integrity is fundamental to the credibility of Supreme Audit Institutions. As SAIs, we are expected to lead by example. Public trust depends not only on what we deliver, but also on how our organizations are governed and the integrity with which we operate in practice.

IntoSAINT (INTOSAI Self Assessment of Integrity) supports this responsibility by holding up a mirror to our organizations. It is based on an understanding that risks to organizational integrity rarely stem from missing rules or are revealed through checklists or compliance reviews. Instead, they arise in weak or poorly informed decisionmaking, in situations of pressure, in informal routines that undermine governance, and in weaknesses in oversight and accountability that are often widely known within the organization but difficult to challenge openly.

IntoSAINT is designed as a structured and facilitated internal dialogue that reframes such concerns from individual behaviour to the organizational conditions that shape it. The process is not about assigning blame or pointing fingers, but about pointing forward. IntoSAINT aims at supporting leadership by bringing vulnerabilities to the surface in a safe and constructive way. Its purpose is to enable learning, reflection and informed management action, while recognising the complexity of organisational governance and management.

Deliberately not a tick-the-box exercise, IntoSAINT aims to generate insight rather than reassurance and helps address integrity risks before they escalate into serious problems or ultimately undermine public trust.

I trust that IntoSAINT will be a practical tool for Supreme Audit Institutions, supporting continuous improvement and helping SAIs to lead by example. I also wish to thank the many experts across regions who, over time, have contributed to refining the methodology; underscoring that IntoSAINT is not static, but continues to evolve through experience and use.

Karl Eirik Schjøtt-Pedersen
Auditor General, NAO Norway
Chair, CBC IntoSAINT workstream

ABOUT THE HANDBOOK

Purpose of the handbook

This Handbook sets out the foundations of the IntoSAINT methodology. It explains how organizational integrity is understood within the framework, the logic of the approach, and how the methodology is intended to be used in Supreme Audit Institutions.

The Handbook describes:

- **the core concepts and principles underpinning IntoSAINT**
- **the four step self-assessment process**
- **roles and responsibilities of management, facilitators and participants**
- **the overall conducting and follow-up of an IntoSAINT process**

The practical tools supporting the full assessment process, including a Facilitator's Guide, are provided separately in a dedicated IntoSAINT toolbox.

Who the handbook is for

The Handbook provides a common reference for facilitators, management, participants and others involved in governance, integrity management, and organizational development, supporting a shared understanding of the IntoSAINT methodology and its purpose.

Quality assurance statement

This Handbook was developed under Quality Assurance Level 3 and builds on guidance material that has been applied and refined since IntoSAINT was adopted by INTOSAI in 2013.

The current edition represents a revised and updated version of earlier handbooks. It was prepared by a team of IntoSAINT experts, drawing on lessons learned and practical experience across diverse regional contexts within INTOSAI. The handbook was also piloted with SAIs in the PASAI and EUROSAI regions and further refined based on feedback from those pilot exercises.

In addition, the draft was shared with members of the CBC Steering Committee – including representatives from all INTOSAI regional organizations, the INTOSAI Development Initiative, the chairs of INTOSAI's four goal committees, the INTOSAI General Secretariat, and the chairs of the CBC's workstreams – for review and input, and all feedback received was duly considered.

Compared to previous editions, this Handbook has been simplified and clarified, with a stronger emphasis on organizational integrity. The guidance more clearly sets out IntoSAINT's focus on the organizational conditions and governance arrangements that shape integrity in practice. This reflects both user feedback and accumulated implementation experience, and reinforces IntoSAINT as a tool for organizational reflection, learning and leadership.

1. INTRODUCTION TO INTOSAINT

IntoSAINT (INTOSAI Self-Assessment of Integrity) is a diagnostic tool developed for Supreme Audit Institutions (SAIs) to evaluate their organizational integrity. In this context, integrity refers to a SAI's ability to carry out its mandate in line with its core values—in a transparent, accountable, and resource-efficient manner.

As model organizations, SAIs are expected to set the standard for good governance and public sector practices, playing a key role in maintaining public trust in government institutions. The integrity of SAIs is fundamental, and IntoSAINT has a clear purpose; to help strengthen integrity within SAIs.

IntoSAINT is a self-assessment tool implemented through a two-day workshop led by trained moderators.[1] It brings together a diverse group of staff from across the organization- representing different roles, levels, genders, and lengths of service—to identify integrity vulnerabilities within the institution's structures, systems, and culture.

The premise is that staff are best placed to recognize the organization's vulnerabilities and assess specific integrity challenges. The focus is on identifying weaknesses that may hinder the institution's ability to uphold its core values.

IntoSAINT offers a structured, collective reflection on how the organization functions and where improvements are needed. While the workshop may result in recommendations for improving integrity management, its core value lies in helping the organization identify potential vulnerabilities, raise awareness, and develop a shared understanding of key integrity issues.

Originally developed in the Netherlands by the Netherlands Court of Audit[2], the tool was updated in 2026 to further reflect the concept of organizational integrity, with a streamlined, simplified modern design to enhance usability and relevance. The update also builds on feedback from SAIs that implemented the previous version.

The methodology is flexible and can be applied across the entire organization, within specific departments, or as a follow-up to earlier assessments.

This handbook outlines the principles, structure, and implementation of IntoSAINT, and refers to supporting materials available for moderators.

[1] In some cases, the workshop may be extended beyond two days to ensure comprehensive discussion and analysis, due to factors such as the need for interpretation, organizational complexity, and other contextual considerations.

[2] Developed together with the Dutch Ministry of the Interior and Amsterdam's Integrity Office, the tool was adapted for international use in 2010 and endorsed by INTOSAI.

2. RELEVANCE FOR INTOSAI

IntoSAINT plays a key role in supporting SAIs in fulfilling their role as model organizations, institutions that lead by example in promoting integrity, transparency, and accountability in the public sector.

Completing an IntoSAINT assessment is also a criterion for SAI-4 in the INTOSAI SAI PMF assessment.

It contributes to the clarity, relevance, and robustness of INTOSAI's standard-setting efforts by offering a practical, systematic and flexible approach to assessing organizational integrity. Rather than prescribing one-size-fits-all solutions, it enables SAIs to reflect on their unique vulnerabilities and select and strengthen appropriate integrity controls.

The tool is closely aligned with the INTOSAI Framework of Professional Pronouncements (IFPP), particularly:

INTOSAI-P 10,
which underscores the critical role of independence in ensuring the credibility and integrity of SAIs.

INTOSAI-P 12,
highlights the responsibility of SAIs to strengthen public sector integrity and demonstrate relevance, value and credibility to citizens and stakeholders.

INTOSAI-P 20,
which sets out the principles of transparency and accountability in SAIs' own governance and operations.

ISSAI 130,
which sets out principles for ethics and integrity that SAIs are expected to apply in their organization.

ISSAI 140,
which sets the organizational requirements that the SAI shall follow for quality management.

ISSAI 150,
which highlights the organizational responsibility of SAIs to ensure auditors have the necessary competences for high-quality and effective audit work.

3. WHY INTEGRITY MATTERS PARTICULARLY FOR SAIS

SAIs play a vital role in holding governments accountable, promoting transparency, and safeguarding public resources. To maintain the trust placed in them, SAIs must uphold the highest standards of integrity within their own organizations. Their credibility depends not only on the quality and independence of their audits but also on how accountably, transparently and effectively they operate.

A key asset of any SAI is its reputation, how it is perceived by the public, stakeholders, and the institutions it audits. This reputation is built over time through consistent professionalism, impartiality, and adherence to high ethical standards. Because SAIs typically do not have enforcement powers, their influence and effectiveness often depend on the credibility and trust they command.

The IntoSAINT methodology requires a clear understanding of why integrity is a strategic concern for Supreme Audit Institutions. SAIs are not more vulnerable to integrity breaches than other public institutions by nature. However, certain features of their mandate and operating environment make the consequences of integrity breaches more significant, and in some cases, more difficult to detect or manage.

By engaging in a self-assessment like IntoSAINT, SAIs show a commitment to continuous improvement and integrity leadership—reinforcing their role as guardians of public trust.

The following factors explain why integrity requires special attention in SAIs:

SAIs operate under high expectations and rely heavily on trust and credibility:

Their influence depends on how their work is perceived by audited entities, decision-makers, and the public. As model institutions, they are expected to demonstrate independence, transparency, professionalism, and accountability—often to a higher standard than other public bodies. This visibility and expectation mean that even the perception of compromised integrity can damage their reputation, weaken their authority, and reduce the impact of their findings and recommendations. To maintain effectiveness, SAIs must not only do everything within their power to avoid integrity breaches but actively demonstrate integrity in all aspects of their operations.

Limited external oversight:

In many countries, SAIs operate independently and are not subject to the same external controls as other public institutions. While this independence is essential for their credibility, it also means that internal integrity systems must be especially robust. Without external checks, the responsibility for preventing and managing integrity risks lies entirely within the institution.

Exposure to sensitive and high-risk processes:

SAIs have inherent vulnerabilities because of the nature of their work. They routinely handle confidential information and make judgments that can have far reaching consequences.

4. CORE FEATURES OF THE INTOSAINT METHODOLOGY

4.1. Integrity is foundational

IntoSAINT is a proactive diagnostic tool designed to help SAIs detect and address integrity issues. Unlike performance assessments like the INTOSAI SAI PMF or peer reviews, it focuses on the systems, values, and culture that underpin good governance and credibility. By concentrating on integrity rather than performance, IntoSAINT helps SAIs understand where risks may arise before they turn into failures or misconduct.

The tool focuses on identifying what may not be working well and where integrity vulnerabilities exist. It is not meant to provide a full evaluation of a SAI's strengths and weaknesses, but rather to highlight areas that may need attention.

4.2. Organizational integrity: A system, NOT a silo

IntoSAINT adopts a comprehensive understanding of integrity, informed by international standards and academic research.

Organizational integrity, as defined by IntoSAINT, refers to an organization's ability to carry out its tasks in accordance with its core values, while achieving its objectives in a transparent, accountable, and resource-efficient manner. It is not simply the sum of individual ethical behaviours, but a systemic quality shaped by the organization's culture, leadership, and institutional frameworks.

Integrity is not a stand-alone task; it is a systemic responsibility that must be embedded throughout the organization. This means that integrity should be reflected in leadership behaviour, integrated into daily operations, and supported by both formal controls and informal cultural norms. The responsibility for organizational integrity should not be siloed into a single unit—such as an ethics office, compliance team, or integrity officer. Just as quality is now understood as something that must be managed across all levels and processes of an organization, integrity must also be systemic.

4.3. A learning process through self-assessment

The workshop is structured as a two-day self-assessment involving up to 20 staff members from across the organization. It is designed to foster learning through structured reflection and open dialogue.

The process centers on two key themes:

Integrity vulnerabilities are factors that may threaten or weaken an organization's ability to achieve its objectives in a manner that aligns with its core values, and that upholds principles of accountability, transparency, and efficient use of resources.

Integrity controls are the mechanisms in place to manage those vulnerabilities, both formal (hard controls) and informal (soft controls).

Participants assess and discuss these themes through a combination of anonymous scoring and facilitated group discussions. The aim is not to produce definitive answers, but to build a shared understanding of where the organization may be vulnerable and how it currently responds to those vulnerabilities.

This structured, participatory approach helps staff think more critically about the conditions that support or threaten integrity in their daily work. It also lays the groundwork for more informed and constructive conversations about what might need to change.

4.4. A focus on prevention

IntoSAINT is preventive. It's not about detecting wrongdoing or assigning blame. Instead, it helps SAIs identify conditions that could lead to integrity problems and take steps to prevent them.

4.4. The role of participants

The quality and credibility of an IntoSAINT assessment depend heavily on the people involved. Participants are not just attendees—they are the core contributors to the process. Their insights, experiences, and perspectives shape the findings and determine the value of the assessment.

For this reason, it is essential that participants are carefully selected.

They should have:

- Relevant knowledge of the organization's systems, culture, and operations.
- Credibility and standing within the organization, so that their contributions are respected and taken seriously.
- A reputation for integrity, ensuring that their input is trusted by peers and leadership alike.
- The ability to reflect critically, engage constructively, and contribute to open dialogue.
- A willingness to speak up, even when it's difficult, raising concerns, sharing observations, and contributing honestly to the discussion.

When participants are seen as trustworthy, competent and courageous, the findings of the workshop carry more weight. This helps ensure that the report is not dismissed or sidelined, but instead becomes a meaningful input into the organization's development.

Equally important is the composition of the group. A well-balanced mix of participants—from different departments, levels, and functions—enriches the discussion and helps uncover integrity issues that might otherwise go unnoticed. Including staff with diverse roles and seniority, especially newer and more junior employees, is essential for capturing a broad range of experiences and perceptions. Their insights often reflect aspects of organizational culture that may not be visible to those in more senior positions.

To foster open and honest dialogue, it is also important to avoid including individuals who have direct reporting relationships within the group. Hierarchical dynamics can inhibit candid contributions, particularly from junior staff who may feel uncomfortable sharing critical reflections about management.

Selecting the right participants is thus not just a logistical step; it is a strategic decision that directly affects the legitimacy and impact of the entire process.

4.5. Confidentiality

Confidentiality is a fundamental principle of the IntoSAINT methodology. While it is up to the organization's management to decide how the final report is used, the process is designed to protect the anonymity and safety of all participants.

No individual statements or identities are linked to specific comments or scores in the report. This safeguard ensures that participants can speak openly and honestly during the workshop without fear of personal repercussions. Moderators are trained to uphold this standard and ensure that the environment remains respectful and secure throughout.

Maintaining this confidentiality is essential—not only to protect individuals, but also to preserve the integrity and credibility of the process itself.

4.6. The role of moderators

Moderators play a critical role in the success of an IntoSAINT workshop. They are not just facilitators—they are guardians of the process, responsible for creating a safe, respectful, and productive environment where participants can speak openly about sensitive issues.

To do this well, moderators must bring a specific set of skills and qualities. They need to:

- Facilitate difficult conversations with care and professionalism, helping participants navigate complex and sometimes uncomfortable topics without fear or defensiveness
- Safeguard participants, ensuring that everyone feels psychologically safe, respected, and heard throughout the process
- Understand organizational dynamics, including how power, culture, and communication flow within institutions
- Be familiar with the environment of a Supreme Audit Institution - its mandate, pressures, and internal challenges—so they can relate to the context and guide discussions meaningfully
- Remain neutral and non-directive, focusing on the process rather than the content, and avoiding any influence over the group's conclusions
- Manage group dynamics, ensuring that all voices are included and that dominant perspectives do not silence others

Moderators must also be able to interpret the results of the anonymous scoring and guide the group in making sense of the findings.

In short, the moderator's role is both technical and human. They must uphold the structure of the methodology while also responding to the emotional and interpersonal dynamics in the room. Their ability to do both is essential to the credibility, safety, and impact of the workshop.

4.7. Thinking in terms of risk

IntoSAINT encourages participants to adopt a risk-based perspective—focusing on conditions that could compromise integrity within the SAI. These are not incidents of misconduct, but vulnerabilities; underlying factors that may increase an organization's exposure to integrity issues over time.

Such vulnerabilities can stem from a variety of sources: internal issues like unclear responsibilities, inconsistent leadership, or a lack of transparency; or external pressures such as political influence, legal complexity, or shifting expectations. Often, these factors interact in subtle ways, making them difficult to detect without deliberate reflection.

4.8. Understanding integrity controls

Alongside identifying integrity vulnerabilities, IntoSAINT also examines how well the SAI is equipped to manage them, not just on paper, but in practice. This involves looking at two types of integrity controls: hard controls and soft controls.

While hard controls provide structure, it is often the soft controls that determine whether those structures are respected and followed. An organization may have all the right policies, but if the culture does not support integrity, those policies may be ignored or undermined.

The IntoSAINT process helps SAIs reflect on both types of controls—how they function and how they interact.

4.9. The relationship between vulnerabilities and integrity controls

In IntoSAINT, vulnerabilities and integrity controls are assessed separately, but they are closely connected. However, the relationship is not one-to-one.

- One vulnerability may require several controls to be managed effectively.
- One control may help reduce multiple vulnerabilities.
- Controls may exist but be too weak or underdeveloped to fully address the vulnerabilities.

Because of this, the relationship between vulnerabilities and controls is complex and overlapping and IntoSAINT does not aim to match each vulnerability to a single control. Instead, it encourages a reflective assessment: looking at whether the overall system of controls—both hard and soft—is strong and mature enough to manage the identified integrity vulnerabilities.

Two main types of integrity controls

These are formal systems such as laws, policies, procedures, internal audits, and reporting mechanisms. They provide structure and define how the organization is expected to operate.

These refer to cultural and behavioural factors, including leadership behaviour, openness, trust, fairness, and shared values. These controls influence how individuals behave and make decisions within the organization

4.10. A reflective report

At the end of the workshop, a self-assessment report is drafted. It summarizes key insights, highlights areas of concern, and may include recommendations for further exploration based on the group discussion. However, the report does not offer fixed solutions. It reflects what participants discussed and is intended to support ongoing dialogue and continuous improvement.

Importantly, the issues raised are often complex and deeply rooted in organizational culture, systems, or leadership dynamics. They are seldom problems that can be solved with quick fixes. While the report may suggest possible next steps, it is not meant to provide a menu of easy actions. Management is encouraged to consider the findings carefully, recognizing that addressing integrity issues often involves complex matters that require thoughtful planning, sustained effort, and engagement across the organization.

However, it is important to note that the report is based on the group's shared perceptions and assessments, which may not always align with objective or externally verified facts. Nonetheless, these insights offer valuable understanding of how integrity is experienced internally.

4.11. The role of the SAI head and top management

The involvement of the SAI Head and top management is critical to the credibility and impact of an IntoSAINT assessment.

Their support signals that integrity is not just a technical issue, but a strategic concern that deserves attention at the highest level.

While the process may at times be uncomfortable—especially when it challenges established assumptions or surfaces difficult truths—it offers a valuable opportunity for leadership to reflect on how integrity is experienced across the organization.

Although top management does not take part in the assessment itself, their role is far from passive. They are expected to create the conditions that make open and honest dialogue possible. This includes protecting the integrity of the process and safeguarding participants who dare to speak up—ensuring that no one faces negative consequences for raising concerns or sharing critical reflections.

This requires a degree of openness and willingness to step outside one's comfort zone. Leaders are not expected to have all the answers, but their readiness to listen, reflect, and engage constructively sets the tone for the rest of the organization. At the same time, they remain responsible for determining how the assessment can serve as a constructive input into broader institutional development. Their role is to ensure that the process is not only heard, but also translated into meaningful follow-up—anchored in the organization's values and strategic priorities.

4.12. Follow-up and management responsibility

IntoSAINT is not a one-size-fits-all solution, and its value depends on what happens after the workshop. While the moderators facilitate the assessment, they are not responsible for follow-up. Once the workshop concludes, it is up to the organization's leadership to take ownership of the findings. Management's commitment to this follow-up is essential for the process to have lasting impact.

There is no single prescribed model for follow-up, but it is strongly recommended that the results be integrated into the SAI's existing risk management framework. This could include incorporating key findings into the institutional risk register or developing a targeted action plan to address identified vulnerabilities.

A formal follow-up process may also be established prior to the assessment, for example when development partner funding is involved. This can include a commitment agreement outlining responsibilities, follow-up milestones, and support for external resources if needed.

While management cultures differ, senior leadership is encouraged to make the findings available within the organization. Sharing results internally supports transparency, strengthens accountability, and helps build a shared understanding of integrity issues across the organization.

4.13 Fostering a culture of integrity

IntoSAINT can be a powerful and sometimes challenging experience. The process invites participants to confront difficult questions about their organization's integrity—questions that may surface uncomfortable truths or raise concerns about accountability and leadership. For some, this can lead to unease, especially in environments where speaking openly does not feel safe.

That's why the methodology is built on confidentiality, respect, and psychological safety. Anonymous scoring and neutral facilitation are not just procedural elements—they are essential safeguards that allow participants to speak honestly without fear of personal consequences.

When these conditions are met, the workshop can lead to a deeper understanding of integrity vulnerabilities and a stronger commitment to addressing them.

Even when the formal conditions are in place, progress is not guaranteed. In environments with low trust and strong resistance to change, the IntoSAINT process may reveal integrity vulnerabilities —but also be met with silence or guarded responses. When fear, fatigue, or institutional pressure dominate, participants may not feel safe enough to speak openly. In such cases, the workshop may not lead to dialogue or change. Its value, if any, lies in exposing the limits of what can be discussed and revealing how deeply integrity issues are embedded and avoided.

5. INTOSAINT – A TOOL FOR THE ENTIRE PUBLIC SECTOR

IntoSAINT was originally developed for the public sector as a self-assessment tool to identify integrity issues and strengthen ethical governance. It was later adapted for Supreme Audit Institutions (SAIs), with adjustments to reflect their specific mandate and audit environment.

Despite this adaptation, the tool remains highly relevant for a wide range of public institutions—such as ministries, regulatory bodies, and local governments—which face similar integrity issues, e.g. conflicts of interest, misuse of public funds, lack of transparency, weak ethical leadership, weak accountability etc.

Using IntoSAINT in these settings requires only small modifications. The core approach- participatory workshops, risk analysis, and action planning, remains the same and is equally effective outside the audit community.

For guidance on how to adapt the tool for broader public sector use, the Facilitator's Guide provides clear instructions and examples of adjustments that may be needed. (Currently being updated).

6. INTOSAINT SELF-ASSESSMENT METHOD – A FOUR STEP APPROACH

IntoSAINT is built around four key steps, each contributing to a deeper understanding of integrity vulnerabilities and the maturity of internal controls.

OVERVIEW OF THE FOUR STEPS OF INTOSAINT

FRAMING ORGANIZATIONAL INTEGRITY

Define what organizational integrity means for the organization by looking at its values, goals and key functions and what is needed to protect integrity in practice.

IDENTIFICATION OF INTEGRITY VULNERABILITIES

Assess how present integrity vulnerabilities are within the organization

ASSESSMENT OF INTEGRITY CONTROLS AND MATURITY

Assess the maturity of integrity controls and identify strengths and weaknesses.

IDENTIFYING ISSUES AND FORMULATING RECOMMENDATIONS

Reflect on identified integrity vulnerabilities in light of existing controls. Highlight the most critical integrity issues and explore possible recommendations to support and strengthen organizational integrity.

STEP 1
Framing organizational integrity

a. Purpose and scope: organizational integrity in IntoSAINT

Step 1 of the IntoSAINT methodology sets the foundation for the integrity assessment. Understanding organizational integrity and its preconditions is essential for identifying vulnerabilities and assessing effective safeguards. This chapter explains how IntoSAINT conceptualizes integrity as a systemic quality and why this understanding is critical for the integrity assessment process.

b. Defining organizational integrity in the context of IntoSAINT

Organizational integrity is defined in IntoSAINT as an institution's ability to carry out its tasks in accordance with its core values, while achieving its objectives in a transparent, accountable, and resource-efficient manner. It is not merely the sum of individual ethical behaviours, but a systemic quality shaped by leadership, institutional culture, and governance structures.

This understanding draws on international standards and research, including definitions from the OECD and UNODC, which emphasize the alignment of institutional behaviour with ethical values and the public interest. Organizational integrity differs from personal integrity by focusing on how institutions create environments that support ethical conduct.

c. Preconditions for integrity: the enabling environment

Integrity in a Supreme Audit Institution is shaped by both external conditions and internal systems.

Externally, the IntoSAINT methodology highlights the importance of an environment that supports integrity. This includes ensuring that institutions have legal and operational independence, access to relevant information, and a clear mandate.

Internally, IntoSAINT emphasizes that integrity is not a separate task or department—it is a quality that runs through the entire organization. It is shaped by leadership, the organizational culture, and the formal systems that guide how decisions are made, how roles are assigned, and how accountability is ensured.

d. External conditions – independence and mandate:

A SAI's organizational integrity is significantly influenced by the external conditions under which it operates. The most critical of these is independence—legal, operational, and financial.

Effective independence means that a Supreme Audit Institution (SAI) can set its own audit priorities, report findings without outside influence, and communicate openly with stakeholders.

To make this possible, certain conditions must be in place:

A clear legal mandate that defines the SAI's role and powers

Full access to the information needed for thorough and objective audits

Freedom from financial or administrative control by the entities it audits

Without this independence, even strong internal systems can be weakened by external pressure. These conditions are essential for maintaining organizational integrity

e. Embedding integrity across SAI processes

Internally, integrity must be embedded across all levels and processes of a SAI—from core audit activities to support functions and strategic governance.

PRIMARY PROCESSES

Integrity in Core Audit Work

The primary processes of a SAI- such as planning, conducting, and reporting audits are the most visible expressions of its mandate. These processes must reflect the highest standards of professionalism and impartiality.

Integrity is demonstrated when audit subjects are selected based on objective criteria, findings are documented transparently, and recommendations are followed up consistently. Risks to integrity may arise if audit planning is influenced by external pressure, if documentation is incomplete, or if follow-up is weak—undermining accountability and public trust.

Embedding integrity in audit work means ensuring that every step—from information gathering to issuing audit opinions—is guided by objectivity, impartiality and professional judgement.

SECONDARY PROCESSES

Integrity in Support Functions

Support processes such as human resources, financial management, and IT systems may not be visible to the public, but they are essential to maintaining organizational integrity.

Integrity is demonstrated through fair and merit-based recruitment processes, transparent and accountable financial management, recognition of performance, and robust IT systems that safeguard sensitive information. Integrity also requires clearly defined accountability mechanisms, ensuring that both leadership and staff are held responsible for their decisions and conduct. Risks to integrity arise when these standards are not upheld. Examples include favouritism in recruitment, misappropriation or misuse of funds, inadequate accountability frameworks, insufficient follow-up on underperformance, and weak data governance. Such practices undermine internal trust and compromise the organization's credibility.

MANAGEMENT AND GOVERNANCE PROCESSES

Integrity in Leadership and Oversight

Management and governance processes define the strategic direction, oversight, and accountability of the SAI. These processes include strategic planning, internal control, performance monitoring, and stakeholder engagement.

Integrity is demonstrated when strategic plans are coherent and realistic, internal audits are active and independent, and leadership plays a decisive role in setting the tone for integrity and professionalism. Leaders are expected to act ethically, demonstrate impartiality, and foster an inclusive and respectful organizational culture. They must be accountable not only for decisions and results but also for the example they set through their conduct. This includes ensuring compliance with governance standards, promoting merit-based practices, and addressing underperformance promptly and fairly.

Risks to integrity may arise from unclear responsibilities, weak internal controls, lack of transparency, or leadership that fails to uphold professional standards. Such weaknesses can lead to inefficiency, favouritism, misuse of resources, and ultimately, loss of institutional credibility.

f. Why this understanding is essential for the IntoSAINT assessment

Understanding organizational integrity and its preconditions is essential for conducting a meaningful integrity assessment. IntoSAINT requires participants to identify vulnerabilities and safeguards across all processes and in the enabling environment. This is only possible when integrity is understood as a systemic quality embedded in institutional structures and supported by enabling conditions.

Step 1 helps participants and facilitators frame the assessment by clarifying what integrity means and how it manifests across the organization.

STEP 2
Identification of integrity vulnerabilities

a. Purpose and scope

Step 2 of the IntoSAINT methodology builds on the institutional understanding of integrity established in Step 1. While Step 1 clarifies what integrity means in an institutional context, Step 2 shifts the focus to identifying the specific conditions that may undermine it.

The purpose of Step 2 is not to investigate wrongdoing, but to assess whether known integrity vulnerabilities derived from international experience and research—are present and relevant in the organization's current context. These factors are not random; they reflect systemic weaknesses that, if left unaddressed, may compromise the institution's ability to act in line with its core values and with transparency, accountability, and resource efficiency.

b. Integrity vulnerabilities in SAIs

To support a structured analysis of integrity vulnerabilities, IntoSAINT applies a framework based on five key themes. Each theme focuses on a specific set of conditions, such as leadership practices, organizational structure, or historical legacies, that are known to create or intensify integrity vulnerabilities even when no misconduct has occurred.

The following sections describe each theme in detail, clarifying how certain conditions may challenge integrity where preventive attention may be needed.

THEME 1

Environmental Complexity

This theme focuses on the external conditions that shape the SAI's operating environment. These are risk factors largely outside the organization's control, but they can significantly affect its ability to function independently and professionally.

In some contexts, SAIs operate within legal frameworks that are overly complex, contradictory, or incomplete. This can create uncertainty about the scope of their mandate or the interpretation of audit standards. Rapid developments in technology may challenge the institution's ability to modernize systems or manage digital vulnerabilities. Excessive administrative requirements imposed by external bodies can slow down operations and reduce flexibility.

Additionally, external actors—such as lobbyists, political figures, or private companies—may attempt to influence the SAI's work. Close relationships with stakeholders or audited entities may raise questions about impartiality. Political intervention, whether direct or indirect, can undermine autonomy and objectivity.

These environmental pressures do not necessarily lead to integrity breaches, but they create conditions that may constrain the SAI's ability to act freely and credibly and affect the SAIs organizational integrity.

THEME 2

Organizational dynamics

This theme examines the internal structure and functioning of the SAI. It focuses on how the organization is designed, how it adapts to change, and how stable and coherent its systems are.

Institutions that are newly established or recently restructured may face challenges in defining roles, building institutional memory, or establishing effective routines. Rigid organizational setups may resist necessary reforms, while frequent changes in legal or procedural frameworks can disrupt continuity and create confusion.

Rapid growth or downsizing can strain coordination, communication, and morale. Outsourcing of core functions—such as audit services—may reduce internal control and accountability, especially if oversight mechanisms are weak. Dependence on external consultants or expertise can dilute institutional ownership of key processes.

Organizational turbulence, such as leadership turnover or unresolved internal conflict, can destabilize operations. In some cases, excessive pressure from external stakeholders regarding performance, efficiency, or budget may lead to shortcuts or compromise professional standards.

These dynamics influence the SAI's ability to uphold consistency, accountability, and resilience in its operations, and may introduce vulnerabilities that threaten its integrity.

THEME 3

Leadership and Management

Leadership is a decisive factor in shaping the integrity climate and strategic direction of the institution. This theme examines how leadership behaviour and management systems influence integrity.

Vulnerabilities may arise when leadership is overly authoritarian, discouraging open dialogue and critical reflection, or when it is indecisive, failing to provide clear direction or address emerging challenges. Ineffective or non-transparent decision-making processes can lead to poor outcomes and reduced accountability. If top-level decisions are made in isolation, without consultation with staff, it can erode trust and weaken institutional cohesion.

A leadership culture focused primarily on reputation may incentivize selective reporting or image management, rather than substantive performance. A lack of accountability among managers, failure to respond to internal concerns, or defensiveness toward criticism can further undermine trust and ethical oversight.

THEME 4

Personnel

This theme considers the conditions affecting staff behaviour, motivation, and well-being. Integrity vulnerabilities may emerge when staff are not held accountable for their performance, when reward systems lack transparency, or when the work environment is psychologically unsafe.

Harassment, excessive workloads, and unclear administrative procedures can erode morale and ethical judgment. Strong group loyalties may override professional standards, and informal power dynamics can obstruct legitimate decisions or delay important initiatives. Personal circumstances—such as side jobs or dependencies—may also affect staff capacity and focus.

These factors influence the integrity of day-to-day operations and the overall ethical climate within the organization. A healthy, fair, and supportive work environment is essential for maintaining integrity across all levels.

THEME 5

Problematic History

An institution's past can shape its present vulnerabilities in subtle but significant ways. This theme explores how unresolved issues, internal narratives, and public exposure of integrity breaches affect current dynamics.

A history of unattended complaints or incidents may signal weak internal accountability and a lack of seriousness in addressing ethical concerns. Persistent gossip and rumours can undermine official communication and create confusion. Public scandals or whistleblower cases may indicate systemic weaknesses and damage the institution's reputation.

Understanding the historical context is essential for identifying blind spots and addressing long-standing vulnerabilities that may continue to influence behaviour and trust. Institutions that fail to reflect on their past may struggle to build a culture of integrity in the present.

c. How Integrity vulnerabilities are assessed in practice

To turn the five themes into actionable insights, the IntoSAINT methodology uses a structured self-assessment questionnaire. This tool allows participants to reflect on whether the conditions described in each theme are present in their organization—and to what extent.

Each participant completes the questionnaire anonymously, rating a series of factors across the five themes based on their own experience and perception. The scoring scale is as follows:

0	1	2	3
Not present	Slightly present	Moderately present	Significantly present

These scores are not intended to measure objective truth. Instead, they capture how integrity vulnerabilities are perceived within the organization. The aim is to surface shared concerns and observations that might otherwise remain unspoken.

Participants score each factor individually. Moderators then facilitate a group discussion to explore the meaning behind the scores, especially where scores are high or where there are large differences in perception (Standard deviation). Participants are encouraged to provide concrete examples to support their assessments. If a score cannot be supported with shared experience or evidence, the group may choose to adjust it to ensure a realistic result. This dialogue helps validate the scores and builds a shared understanding of the organization's integrity landscape.

The results are then synthesized into an integrity vulnerability profile—an overview of the conditions that may increase vulnerability to integrity breaches. This includes both the scores for each theme and an overall indication of the integrity vulnerability level for the organization as a whole.

THEME	AVERAGE SCORE	VULNERABILITY LEVEL
Environmental Complexity	[score]	☐ Low ☐ Medium ☐ High
Organizational Dynamics	[score]	☐ Low ☐ Medium ☐ High
Leadership and Management	[score]	☐ Low ☐ Medium ☐ High
Personnel	[score]	☐ Low ☐ Medium ☐ High
Problematic History	[score]	☐ Low ☐ Medium ☐ High
Overall Integrity Vulnerability	[overall score]	☐ Low ☐ Medium ☐ High

The scores indicate whether the organization faces low, medium, or high integrity vulnerability in each area and is based on the following thresholds:

AVERAGE SCORE	VULNERABILITY LEVEL
Average ≤ 0.8	Low
0.8 < Average ≤ 1.6	Medium
Average > 1.6	High

The integrity vulnerability profile is incorporated into the self-assessment report and forms the basis for assessing the organization's overall integrity challenges in Step 4.

STEP 3
Assessment of integrity controls and maturity

a. Purpose and scope

Step 3 of the IntoSAINT methodology focuses on identifying and evaluating the integrity controls that help an organization manage its integrity vulnerabilities.

These controls—both formal and informal—support the organization's ability to act in line with its values and to achieve its objectives in a transparent, accountable, and resource-efficient manner.

b. Categories of integrity controls

IntoSAINT distinguishes between two main types of integrity controls: hard integrity controls and soft integrity controls.

Both types of controls are essential and together they form the foundation of a strong integrity system. Hard controls may be well-designed but ineffective if not supported by a culture of integrity. Conversely, a strong ethical culture may be undermined by the absence of clear rules and accountability mechanisms.

The hard controls are classified in line with how control activities are defined in financial audit standards.

Two main types of integrity controls

These are formal systems such as laws, policies, procedures, internal audits, and reporting mechanisms. They provide structure and define how the organization is expected to operate.

These refer to cultural and behavioural factors, including leadership behaviour, openness, trust, fairness, and shared values. These controls influence how individuals behave and make decisions within the organization

c. Assessment method

The maturity of integrity controls is assessed through a structured questionnaire completed during the workshop. Participants evaluate both hard and soft controls based on their own experience and perception. The scoring scale reflects the degree to which each control is present and functioning in practice. A four-point scale is used to reflect the level of maturity:

LEVEL	DESCRIPTION
x	**DON'T KNOW** No information or awareness of the topic
0	**DOES NOT EXIST**
1	**WRITTEN DOWN:** Exists on paper but not being applied
2	**PARTIALLY WORKING:** Some parts are in place, but not fully effective
3	**WORKING WELL:** Consistently applied/ practiced and effective

This scoring is not scientific or externally validated. It is designed to support internal reflection by surfacing shared perceptions and identifying areas where controls may be weak, underdeveloped, or inconsistently applied.

d. Structure of the integrity control system

The questionnaire is organized into five categories of hard controls and three categories of soft controls:

Hard Controls:

- → **Control Environment** – Legal framework, independence, ethical standards
- → **Risk Assessment** – Processes for identifying and analyzing operational and strategic risks
- → **Control Activities** – Rules and procedures guiding daily operations
- → **Information and Communication** – Mechanisms for sharing relevant information and ensuring transparency and clarity in its operations.
- → **Monitoring** – Internal and external reviews of the functioning of the organization.

Soft Controls:

- → **Leadership and Role Modelling** – Behaviour and tone from leadership
- → **Openness, Trust, and Accountability** – Conditions for psychological safety and fairness
- → **Values and Learning** – Shared norms, reflection, and continuous improvement

Each category includes a set of reference measures based on international good practices. These serve as prompts for discussion and help participants assess how well integrity is embedded in both systems and culture.

e. Interpreting the results

Scores are aggregated to produce average values for each control category. An overall average score is also calculated.

The overall score reflects the maturity level of the integrity control system:

0 ≤ average ≤ 1 indicates **low maturity**
1 < average ≤ 2 indicates **medium maturity**
2 < average ≤ 3 indicates **high maturity**

These results provide an indication of where there might be challenges in the integrity control system. They provide a structured basis for reflection and dialogue, helping the organization understand how well it is equipped to manage integrity risks and where further development may be needed.

f. The relationship between vulnerabilities and controls

The relationship between integrity vulnerabilities and controls is not one-to-one. A single vulnerability may require multiple controls to be managed effectively, and one control may help mitigate several vulnerabilities. Some controls may exist but be too weak or inconsistently applied to have the intended effect.

It is also important to recognize that not all vulnerabilities can be addressed through control measures alone. Some vulnerabilities may be rooted in deeper cultural or structural issues that require long-term attention.

Conversely, the absence of a control—or the presence of a control that does not function as intended—can itself be considered an integrity vulnerability. In this sense, the assessment of controls is also a way of detecting additional integrity vulnerabilities—especially those that may not have been fully captured in Step 2. Hence, Step 3 of the IntoSAINT methodology not only assesses the presence and maturity of integrity controls, but also helps identify vulnerabilities that arise when those controls are weak, unknown, or ineffective.

To sum up:

- → **STEP 2** examines integrity vulnerabilities through five thematic lenses: environmental complexity, organizational dynamics, leadership and management, personnel, and problematic history. These themes help identify conditions that may increase the likelihood of the organization acting in ways that are not aligned with its values.
- → **STEP 3** assesses the maturity of integrity controls—both formal and informal mechanisms that are intended to manage those vulnerabilities. When controls are weak, absent, or not functioning as intended, they may themselves represent integrity vulnerabilities or contribute to existing vulnerabilities.

Together, these two steps offer a fuller picture of the organization's integrity landscape. Step 2 highlights where vulnerabilities may arise, while Step 3 reveals how well the organization is equipped to respond. This dual perspective supports a nuanced and practical understanding of integrity issues —and insights gained in step 2 and 3 form the basis for Step 4, where participants identify key integrity issues and formulate recommendations.

STEP 4
Identifying issues and formulating recommendations

Step 4 brings together the insights from the previous steps. Participants reflect on the identified vulnerabilities and the maturity of existing integrity controls to pinpoint key integrity challenges that warrant attention.

This step is not about solving problems, but about framing them, highlighting areas where integrity may be at risk and where further action is needed.

Assessing integrity issues in a SAI the following issues will typically come to the fore:

Political and institutional pressure that may threaten independence

Internal misconduct, such as favouritism, nepotism or misuse of authority.

Weak internal accountability, where unclear responsibilities allow poor decisions to go unchecked.

Management challenges, including ineffective leadership, lack of strategic direction, innovation and risk management

Complacent culture, where a strong reputation leads to overlooked risks or outdated controls.

Blind spots, where routine, assumptions, or lack of internal challenge prevent recognition of emerging risks.

Limited transparency, which can erode public trust if SAIs do not model openness themselves.

Lack of self-assessment, which prevents early detection of vulnerabilities.

It is important to recognize that integrity challenges are often complex and rooted in organizational culture, systems, or leadership dynamics. The workshop group is not expected to provide definitive solutions. Participants may not have the mandate, expertise, or full information needed to design effective interventions. There is also a risk that management may focus on the most visible or easiest recommendations, rather than those that require deeper change.

To avoid this, recommendations can be kept generic and strategic, pointing to areas that require attention without prescribing specific actions.

This type of recommendations helps shift the focus from isolated fixes to systemic follow-up. They also reinforce the principle that management must own both the issues and the response. This includes validating the findings, prioritizing actions, and integrating them into existing frameworks.

Without structured follow-up, the assessment risks becoming a one-off exercise. Integrity challenges require sustained attention, cross-functional engagement, and leadership commitment to translate insights into meaningful change.

Examples of generic recommendations include:

Develop a structured follow-up plan to address identified vulnerabilities.

Ensure that integrity challenges are considered in strategic planning and risk management processes.

Establish clear ownership and accountability for follow-up actions.

ANNEXES

ANNEX 1: QUESTIONNAIRE SELF-ASSESSMENT OF INTEGRITY VULNERABILITIES

Integrity vulnerabilities

Within the framework of this assessment method, integrity vulnerabilities are divided into the following five clusters as a common point of reference:

- Environmental complexity
- Organizational dynamics
- Leadership and Management
- Personnel
- Problematic history

Please evaluate the list of vulnerabilities shown below, which could pose threats to integrity in your institution. Assign a score to each factor (seen from a negative perspective) considering the extent to which it materializes in the organization. The ratings given range from 0 to 3, according to the following criteria:

SCORE	INCIDENCE IN THE INSTITUTION
0	Not present
1	Slightly present
2	Moderately present
3	Significantly present

TABLE: VULNERABILITY AREAS WITH SCORE COLUMN

CATEGORY	ELEMENT	SCORE
Environmental complexity	**1.1 ICT Innovation –** The organization has difficulties keeping up with the rapidly evolving ICT development	
	1.2 Complex legislation – Legal framework that is complex, contradictory and with significant gaps.	
	1.3 Excessive external bureaucracy – Excessive administrative requirements complicating the operations of the organization	
	1.4 Lobbying – Actions performed by external groups trying to influence operations of the organization	
	1.5 Close relationships – Close relationships with clients and stakeholders of the organization that cast doubt on the impartiality and professionalism of the institution.	
	1.6 Engagement with private companies – Engagement with private companies complicating the operations of the organization	
	1.7 Political influence / intervention – Interventions of political actors in the operations of the organization that put into question its autonomy, objectiveness, and professionalism.	

CATEGORY	ELEMENT	SCORE
Organizational dynamics	**2.1 New organization** – The organization is recently created, modified or has a new inexperienced leadership	
	2.2 Rigid organization – Lack of organizational dynamics and low response to change in the external environment	
	2.3 Frequently changing legal framework and standards – The regulatory framework changes frequently altering organizational stability	
	2.4 Rapid growth or downsizing – Substantial increase or reduction of staff in the organization, which affects its efficiency, productivity, coordination, communication, motivation and ability to fulfil its mandate.	
	2.5 Outsourcing of audit services – Process in which the operation of the organization moves from the public to the private sector, which provides an opportunity for officials to personally benefit	
	2.6 Need for external expertise – The organization is dependent on consultancy or external expertise for its development.	
	2.7 Organizational turbulence – Recent turbulent situations resulting in instability and uncertainty within the organization	
	2.8 External pressure – Excessive external pressure (from stakeholders and political actors) in respect to performance, operational efficiency and budget, which undermines professionalism, quality and efficiency of the organization	
Leadership and management	**3.1 Authoritarian leadership** – Authoritarian leadership discourage an internal culture of free expression and critical debate	
	3.2 Indecisive leadership – Indecisive top management failing to set strategic direction, avoiding conflicts at all costs	
	3.3 Ineffective management processes – Top management processes are cumbersome and/or non-transparent leading to inefficient decision making	
	3.4 Isolated management – Top management's decisions are taken without due consultations with middle management and concerned staff	
	3.5 Biased reporting incentives – Top management is preoccupied with upholding reputation and prestige with the risk of selective performance information	
	3.6 Compromised professional integrity – Failing to meet required standards leading to errors and poor performance, e.g. baseless conclusions and or unsubstantiated claims in reports	
	3.7 Lack of accountability – Managers in the organization are generally not held accountable for results and decisions and behaviour in the organization	
	3.8 Ignoring advice/signals – Top management tends to ignore signs of violations to integrity in the organization	
	3.9 Defensive response to criticism or complaints – Defensive or reactionary attitude from top management towards complaints and concerns raised by staff	

CATEGORY	ELEMENT	SCORE
Personnel	**4.1 Lack of accountability** – Staff in the organization are generally not held accountable for their performance	
	4.2 Inconsistent rewards and career prospects – Staff in the organization are not rewarded based on their performance and objective and transparent criteria	
	4.3 Poor psycho- social working environment – Due to e.g. remote work, toxic culture, etc.	
	4.4 Harassment – Various forms of harassment, including sexual harassment, bullying, and other unwanted or offensive behaviour	
	4.5 Elevated workloads – Excessive or unevenly divided workload	
	4.6 Lack of administrative and budgetary clarity – Administrative and budgetary systems and procedures are unclear, cumbersome and or/ inadequate	
	4.7 Group loyalty – Strong group loyalties trump professional judgement	
	4.8 Power to obstruct – Vested interest and informal power or dominance can delay or prevent decisions or projects/activities to be implemented	
	4.9 Private preoccupations affecting productivity and/or integrity – Staff have private preoccupations unrelated to the organization which affect productivity and/or integrity, such as additional paid employment, significant voluntary or community responsibilities, dependencies etc.	
Problematic history	**5.1 Unattended complaints and previous incidents** – Recurrent complaints about breaches of integrity of or within the organization. Management is not perceived to take internal integrity matters seriously in our recent history.	
	5.2 Gossip and rumours – Internal official communication and management decisions are constantly challenged and contradicted by gossip and rumours in the organization	
	5.3 Signals / whistleblowers – Presence of situations or scandals about breaches of integrity and that are made public outside the organization.	

ANNEX 2: QUESTIONNAIRE SELF-ASSESSMENT OF INTEGRITY CONTROLS

Integrity control system

Implementing formal and informal mechanisms to ensure integrity is maintained in every aspect of an organization is essential. The IntoSAINT methodology distinguishes between two types of integrity controls: hard controls, which include formal systems, structures, and procedures, and soft controls, which refer to cultural and behavioural factors such as leadership, openness, trust and shared values.

Hard and soft controls that address matters that impact organizational integrity, serve different but complementary purposes. Hard controls provide the formal framework for how the organization functions, while soft controls shape the internal culture and influence how people behave and make decisions in practice. Though less visible, soft integrity controls are critical for embedding integrity in daily operations and can significantly support or undermine organizational integrity.

Together, these controls create the structure and culture needed to uphold integrity by ensuring that the organization operates in a transparent, accountable, and resource-efficient manner, in line with its values.

This questionnaire focuses on selected controls identified in the IntoSAINT framework as particularly important for assessing and strengthening an organization's integrity control system.

Hard controls related to integrity matters

Hard controls related to integrity matters form the structural backbone of an organization's integrity system. They consist of formal mechanisms designed to ensure that operations are aligned with integrity principles. This section of the questionnaire covers five key categories:

- **Control Environment**: The legal and organizational framework that defines the mandate, independence, and responsibilities for upholding integrity.
- **Risk Assessment**: Processes to identify and assess risks that could compromise transparency, accountability, or responsible use of resources.

Control Activities: Formal rules and procedures that prevent, detect, and address integrity breaches in daily operations.

- **Information and Communication**: Mechanisms to ensure integrity-related information is shared clearly, both internally and externally.
- **Monitoring**: Regular reviews and audits to evaluate the effectiveness of integrity controls and support continuous improvement and strengthening of integrity culture.

Please complete the questionnaire by scoring the maturity level of each measure in your SAI based on your own perception. No additional research within your organization is required.

LEVEL	CRITERIA
x	**Don't know** : No information or awareness of the topic
0	**Does not exist**
1	**Written down**: Exists on paper but not being applied
2	**Partially working**: Some parts are in place, but not fully effective
3	**Working well**: Consistently applied/practiced and effective

TABLE: CONTROL AREAS WITH SCORE COLUMN

CATEGORY	SUBCATEGORY	ELEMENT	SCORE
1. Control Environment	1.1 SAI Legal Framework	**1.1.1** Existence and independence of the SAI embedded in the Constitution	
		1.1.2 Independence of SAI heads and staff, including security of tenure and legal immunity in the normal discharge of their duties	
		1.1.3 Broad mandate and full discretion in the discharge of SAI functions	
		1.1.4 Unrestricted access to information	
		1.1.5 Right and obligation to report on the SAIs work and freedom to decide content and timing of audit reports	
		1.1.6 Financial and managerial/administrative autonomy and availability of appropriate resources	
	1.2 Professional SAI Standards and regulations	**1.2.1** SAI not involved in the management of the organization it audits	
		1.2.2 Communication with Executive does not compromise independence or create perceptions of influence	
		1.2.3 Prevention of undue influence from external environment (lobby groups, politicians etc.)	
		1.2.4 Job rotation to ensure personnel do not develop close relationships with entities they audit	
	1.3 Code of Ethics	**1.3.1** Code of ethics covering trust, integrity, independence, objectivity, professional secrecy, due care, competence	
		1.3.2 Employees have been involved in the formulation of the code of ethics and standards	
		1.3.3 Training on the Code of Ethics is part of professional development program for all staff	
		1.3.4 Procedures available for identification and analysis of ethical risks	
		1.3.5 Mechanism/contact point within the organization for raising integrity or ethical concerns	

CATEGORY	SUBCATEGORY	ELEMENT	SCORE
2. Risk Assessment	**2.1 Vulnerability Analysis: Regulations, policies and guidelines to ensure**	**2.1.1** Regular vulnerability/ risk analysis for integrity risks is completed	
		2.1.2 In-depth analysis occurs for vulnerable areas and roles/positions	
3. Control Activities	**3.1 Integrity Legislation, policies and guidelines that include**	**3.1.1** Fixed and transparent procedures for dealing with job application to ensure fairness and consistency	
		3.1.2 Job descriptions for all staff members including management	
		3.1.3 Prevention of "revolving door" arrangements where staff move between public and private sectors in ways that could compromise integrity	
		3.1.4 Proper management of external positions & financial interests to prevent conflict of interests	
		3.1.5 Regulations on acceptance of gifts to avoid undue influence	
		3.1.6 Protection of sensitive information e.g. signing of Declarations of confidentiality by staff	
		3.1.7 Addressing undesirable conduct within the organization to maintain a professional environment	
		3.1.8 Clear lines of responsibility and accountability to ensure everyone knows their duties and can be held accountable	
		3.1.9 Time recording system for actual working hours	
		3.1.10 A system for clear expense and travel claim	
		3.1.11 "Four-eyes principle" application to critical decisions and transactions to enhance oversight and accountability	
		3.1.12 A system for monitoring staff competence development to ensure continuous improvement	
		3.1.13 Monitoring and follow-up of overtime	
		3.1.14 Regular job satisfaction surveys or similar, e.g. culture perception surveys	
		3.1.15 Transparent criteria for promotion and salary increases	
		3.1.16 Regular performance evaluations and transparent feedback for staff	
		3.1.17 Regular performance evaluations and transparent feedback for management	
		3.1.18 Screening of external contractors to ensure they meet integrity standards	
	3.2 Physical & ICT Security: Regulations, policies and guidelines available	**3.2.1** Providing adequate physical protection of organizational assets (e.g., locks and safes)	
		3.2.2 Providing ICT security to safeguard information integrity (e.g. access authorization)	

CATEGORY	SUBCATEGORY	ELEMENT	SCORE
	3.3 Response to Integrity Violations: Regulations, policies and guidelines available	**3.3.1** Ensuring notification procedure for employees to report suspected violations (whistleblower protection)	
		3.3.2 Ensuring procedures for handling information and complaints from external sources	
		3.3.3 Ensuring procedures for investigating suspected integrity violations	
		3.3.4 Ensuring that suspicions of criminal offences are always reported to the public prosecutor or the police	
		3.3.5 Ensuring that incidents are evaluated and discussed with staff involved to learn from mistakes and prevent recurrence	
4. Information & Communication	**4.1 Accountability & Transparency: Regulations, policies and guidelines available**	**4.1.1** Ensuring that SAI's mandate, role, responsibilities, organization, mission, strategies, audit manuals, procedures and criteria are public	
		4.1.2 Ensuring that SAI's audit findings and conclusions are subject to contradictory procedures (Auditees have the opportunity to respond to audit findings before final conclusions are made)	
		4.1.3 Ensuring that SAI accounts are public & subject to external audit or parliamentary review	
		4.1.4 Ensuring that outsourcing and sharing audit activities with external entities are performed under precise rules, clear and well-defined quality standards	
		4.1.5 Ensuring that Codes of ethics are public	
		4.1.6 Ensuring that SAIs issue reports publicly on audit findings and SAI management and performance	
		4.1.7 Ensuring effective communication with external stakeholders, including regulatory bodies, media and the public	
		4.1.8 Ensuring high standards for documentation & record-keeping	
5. Monitoring	**5.1 Auditing & Monitoring: Regulations, policies and guidelines available**	**5.1.1** Ensuring regular independent reviews of the organizational integrity (including effectiveness and efficiency of SAI's processes for risk monitoring, control and governance)	
		5.1.2 Regular internal audit of integrity systems	
		5.1.3 Regular management evaluation of organizational integrity	

Soft Integrity Controls

While formal structures and procedures are essential for safeguarding integrity, they are not enough on their own. The behaviour, mindset, and culture within an organization—known as soft controls—play a critical role in ensuring integrity is upheld in practice.

Soft integrity controls shape how people interact, make decisions, and respond to ethical challenges. They include leadership behaviour, openness, accountability, psychological safety, and shared values, all of which influence whether integrity is truly embedded in daily operations.

This section assesses the maturity of these cultural and behavioural factors. Please score each measure based on your perception of how well these soft integrity controls are present and practiced in your organization.

LEVEL	CRITERIA
x	**Don't know**: No awareness or information about this aspect of integrity culture.
0	**Does not exist**: This behaviour or cultural element is not present in the organization
1	**Written down**: It is mentioned in policies or values, but not visible in daily behaviour
2	**Starting**: Some practices or behaviours are emerging, but not yet consistent
3	**Working well**: This is consistently practiced and embedded in the organizational culture.

CATEGORY	ELEMENT	SCORE
1. Leadership and Role Modelling	**1.1:** Management actively promotes the importance of integrity through communication and behaviour	
	1.2: Managers lead by example and comply with integrity regulations and codes of conduct.	
	1.3: Ethical leadership is a key criterion in leadership selection and development	
	1.4: Management consistently responds appropriately to integrity issues	
	1.5: Middle managers reinforce integrity messages from leadership	
	1.6: Middle managers are seen as credible and consistent in their ethical behaviour	
	1.7: Staff related decisions (e.g., promotions, workload, recognition) are perceived as fair across the organization	
	1.8: Rules are applied consistently across all levels within the organization.	
2. Openness, Trust, and Accountability	**2.1:** Staff feel safe discussing ethical dilemmas, reporting concerns and acknowledging mistakes.	
	2.2: There is sufficient opportunity to express criticism constructively.	
	2.3: There is a culture of holding others accountable for their conduct.	
	2.4: Accountability is applied fairly, regardless of position or seniority.	

CATEGORY	ELEMENT	SCORE
3. Values and learning	**3.1:** Integrity is part of the organization's core values.	
	3.2: Ethical behaviour is a shared expectation and a visible part of our daily work practise and culture	
	3.3: Respect is shown to individual differences so that diversity of thought is encouraged and a high standard of behaviour is expected in all relationships	
	3.4: Integrity criteria are included in role descriptions and reflected in how performance is measured and rewarded	
	3.5: The organization regularly reflects on its integrity culture and provides training to support awareness and continuous improvement.	
	3.6: It is widely recognized that meaningful action is taken when integrity issues are raised	
	3.7: Integrity-related incidents are reviewed to identify lessons learned.	
	3.8: Rule-bending is not tolerated; staff are expected to act with integrity and sound judgment.	
	3.9: Formal policies guide decisions and take precedence over informal habits or unwritten rules.	

ANNEX 3: SUPPORTING MATERIALS

To support practical implementation, IntoSAINT is accompanied by a comprehensive set of materials that that together ensure a structured, consistent, and high quality assessment process. The supporting materials form an integrated package that together support preparation, facilitation, analysis, and reporting throughout the IntoSAINT assessment and are designed to function as practical working tools throughout the process.

Facilitator's Guide – How to Run an IntoSAINT Integrity Assessment.

The Facilitator's Guide provides practical guidance for facilitators responsible for delivering an IntoSAINT assessment. It translates the methodology into practice by describing how the assessment is prepared, how the two day workshop is facilitated, how the four steps are conducted, how questionnaires are used, and how results are documented and presented to top management.

In addition, IntoSAINT is supported by standard materials that assist with:

- preparing and organising the assessment,
- facilitating the workshop,
- reporting results and engaging in dialogue with top management,
- supporting reflection and learning on organizational integrity, and
- safeguarding confidentiality and the integrity of the assessment process.

Supplementary reference material is also provided, including explanatory notes on integrity vulnerabilities and integrity controls, which support a common understanding of key concepts and assessment criteria.

INTOSAI Capacity Building Committee | INTOSAI CBC

https://www.intosaicbc.org